Nama: Aga Wira Julyansyah (09011381722099)
Sistem Komputer 4A

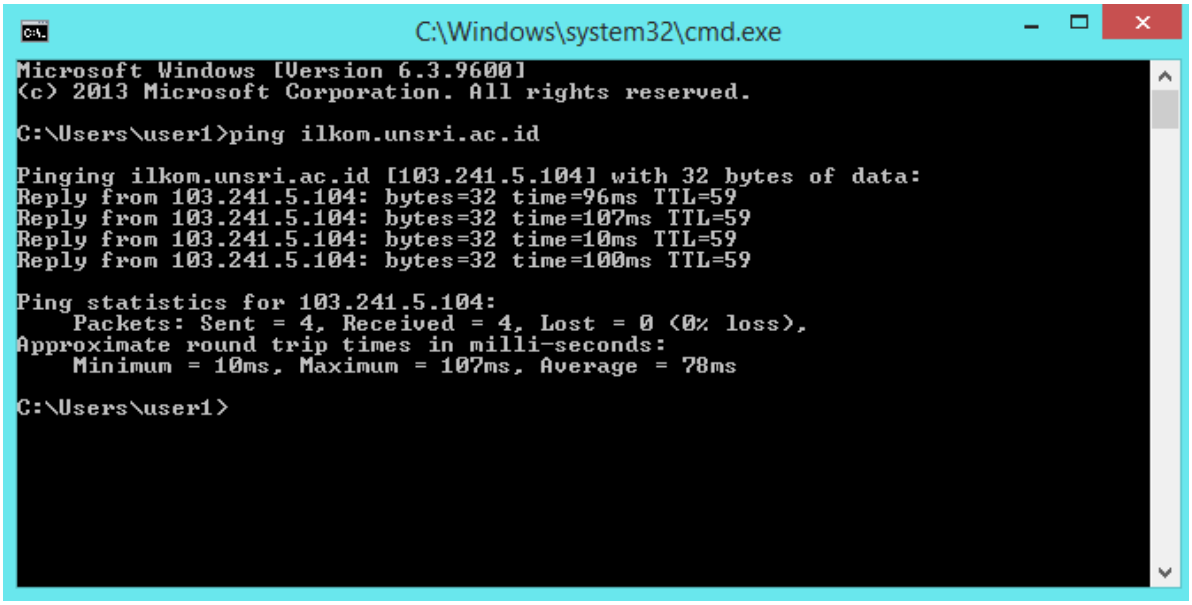
Tugas Komunikasi Data

Menganalisis Packets menggunakan Wireshark

Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network Administrator untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang Anda kelola. Wireshark menggunakan interface yang menggunakan Graphical User Interface (GUI).

Wireshark mampu menangkap paket-paket data yang ada pada jaringan tersebut. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa.

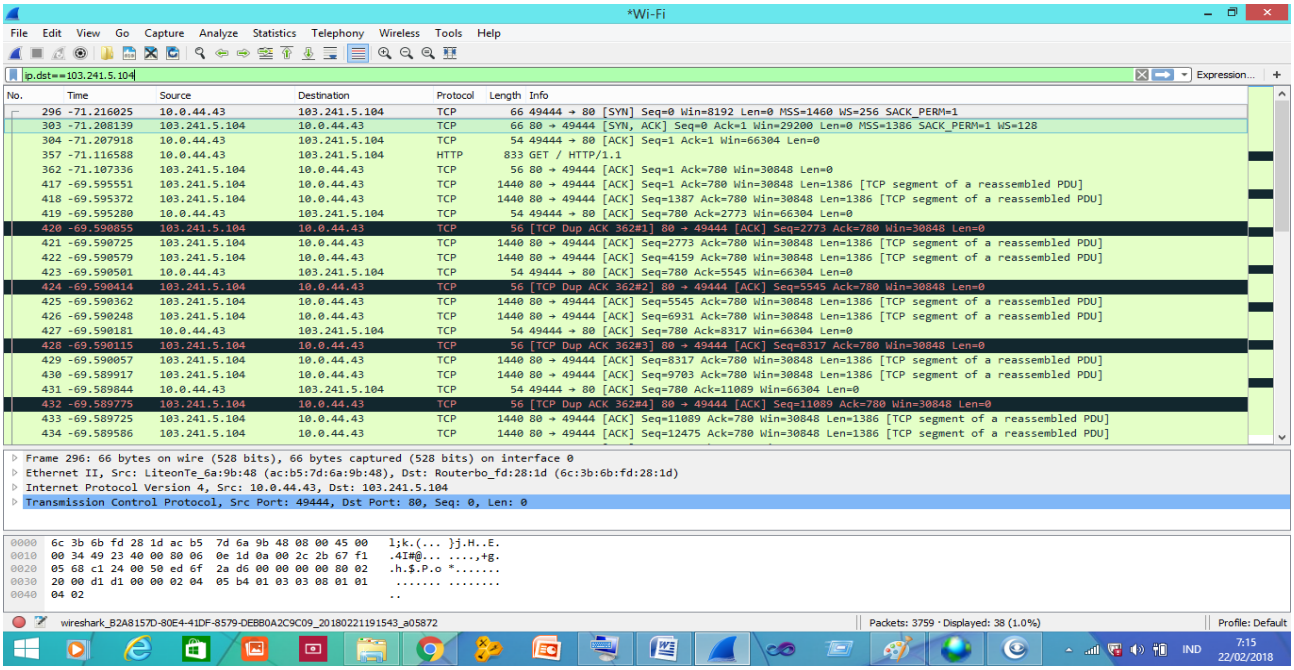
Saat ini saya akan menganalisis packet protokol yang ter capture saat membuka situs website (ilkom.unsri.ac.id), sebelum itu kita harus membuka terlebih dahulu buka webnya lalu mengetahaui ip dari ilkom.unsri.ac.id di CMD, seperi gambar:



saya akan menganalisis packet protokol yang ter capture saat membuka situs website (ilkom.unsri.ac.id).

Setelah itu, buka wireshark lalu meng-capture proses dan klik stop untuk menghentikan capture. Berikut adalah hasil sebagian tampilan yang telah di-capture. Bisa kita lihat pada gambar berikut ini:

berikut hasil analisa jaringan yang ter capture:



Setelah membuka wireshark menekan wifi yang ada pada wireshark maka akan timbul capture saat membuka tab website (ilkom.unsri.ac.id). Saya akan menjelaskan protocol yang tertangkap pada saat membuka (ilkom.unsri.ac.id):

Menggunakan **TCP:**

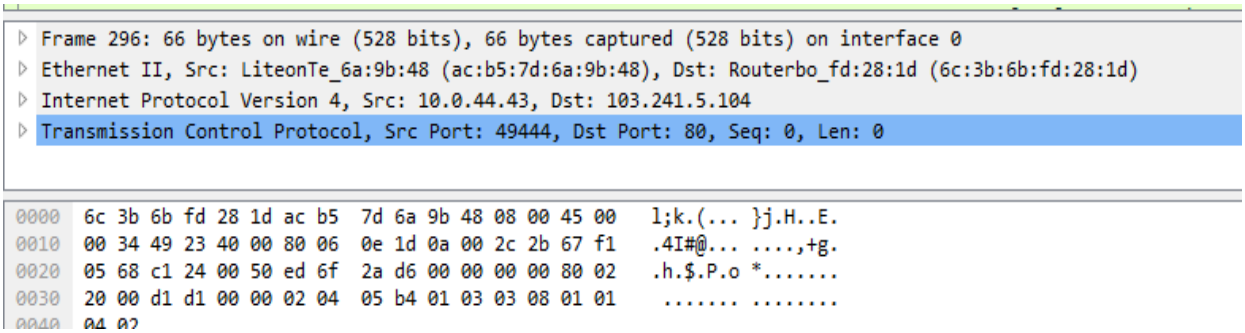
```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Wed, 21 Feb 2018 12:17:16 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: wfvt_613827590=5a8d634b19850; expires=Wed, 21-Feb-2018 12:47:15 GMT; Max-Age=1800; path=/; HttpOnly
Referrer-Policy: unsafe-url
x-frame-options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Link: <http://ilkom.unsri.ac.id/wp-json/>; rel="https://api.w.org/"
Content-Encoding: gzip
```

Pada baris pertama dapat disimpulkan bahwa versi http yang dipakai ialah /HTTP/1.1, di baris kedua host yang sedang dibuka atau web yang sedang dibuka ialah ilkom.unsri.ac.id, lalu di baris ketiga diketahui bahwa koneksi sedang berjalan atau aktif (keep-alive). Kemudian dibaris kelima browsing menggunakan Mozilla versi 5.0 dan Chrome dan safari. Lalu accept encoding menggunakan format gzif dan deflate. Accept languagenya ialah ID [Indonesia]. Dan pada baris yang menjelaskan cookies artinya sedang berjalan.

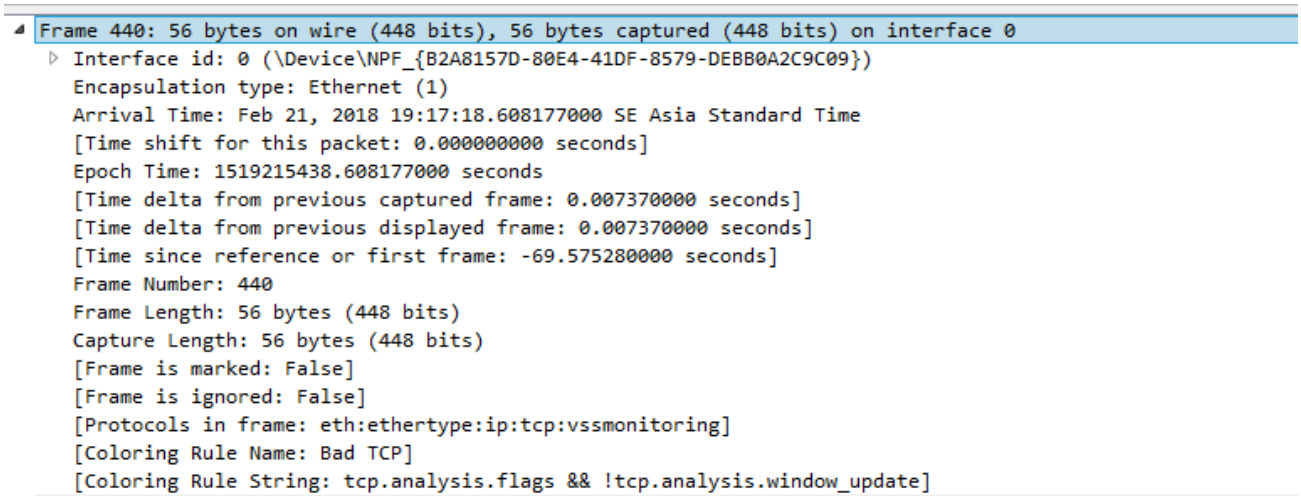
Selanjutnya:

Pada baris kedua server yang kedua menggunakan server basic ubuntu. Dan waktunya adalah hari Rabu, 21 Februari 2018. Lalu koneksi masih berjalan (keep-alive). Lalu conten encoding menggunakan format gzif.

Selanjutnya:

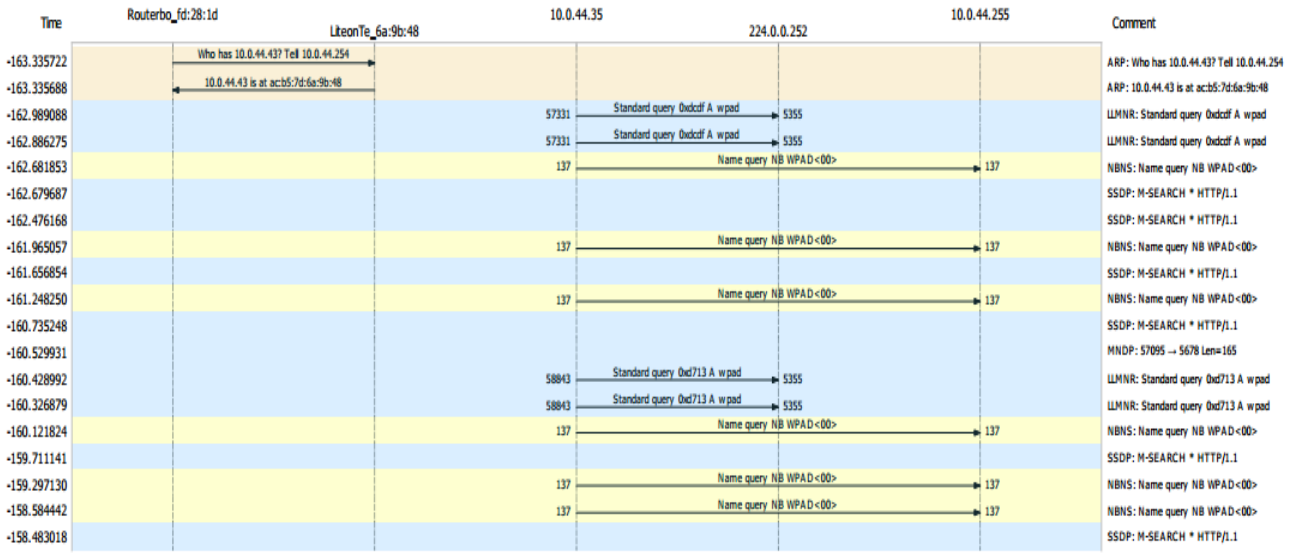


Pada baris pertama disebutkan frame, frame pada wireshark adalah jaringan (network) 66 bytes on wires dan captured (528 bits) . port 494444, dapat diliat dari gambar:



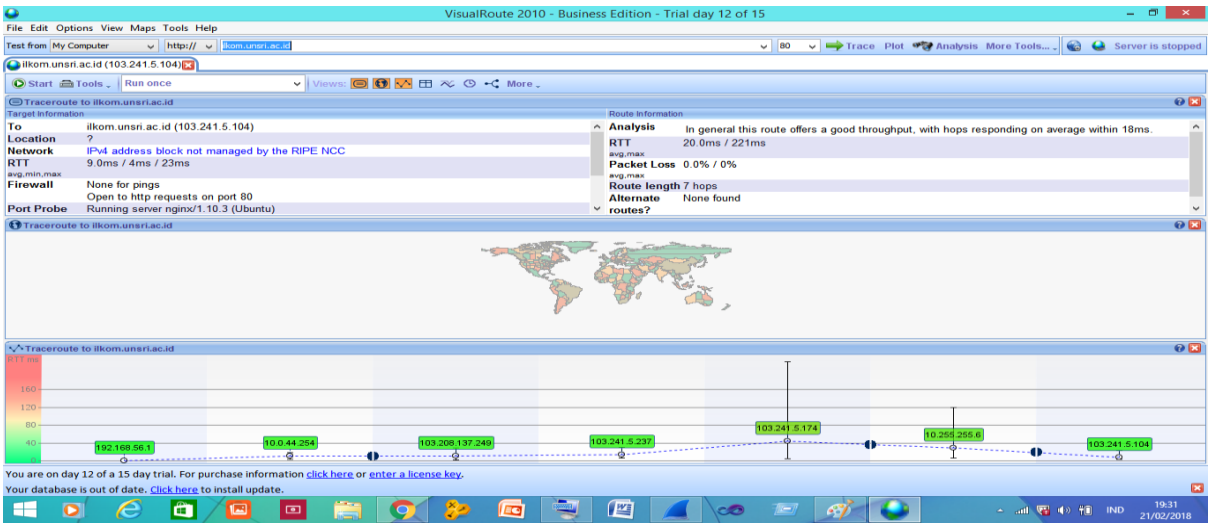
FLOWGRAPH pada Wireshark (ilkom.unsri.ac.id)

Lihat flow graphnya dengan cara pilih menu statistics>flow graph>klik ok.



Gambar diatas merupakan flow graph dari proses berlangsungnya ssh. Pada flow graph ini kita dapat melihat secara detail bagaimana proses enkripsi tersebut satu per satu. Selain ACK, Pada gambar terdapat encrypted request dan encrypted response . Encrypted request dan encrypted response itu adalah data-data hasil enkripsi yang tidak bisa dilihat oleh sembarang orang.

Menggunakan Visual Route



Traceroute to ilkom.unsri.ac.id:

Hops	Loss	IP	Name	Location	Tzone	Avg ms	Min ms	Max ms	Network
0	0	192.168.56.1	user	-	-	0.0	0	0	[Local Network]
1	0	10.0.44.254	-	-	-	11.0	4	19	[Local Network]
2	0	103.208.137.249	ip-103-208-137-249.unsri.ac.id	-	-	12.0	3	29	IPv4 address block not managed by the RIPE NCC
3	0	103.241.5.237	ip-103-241-5-237.unsri.ac.id	-	-	14.0	7	31	IPv4 address block not managed by the RIPE NCC
4	0	103.241.5.174	ilkom-idl.unsri.ac.id	-	-	45.0	5	221	IPv4 address block not managed by the RIPE NCC
5	0	10.255.255.6	-	-	-	29.0	7	120	[Local Network]
6	0	103.241.5.104	ilkom.unsri.ac.id	-	-	9.0	4	23	IPv4 address block not managed by the RIPE NCC

Diliat dari Colasoft Capsa:

Capsa adalah penganalisa jaringan portabel untuk LAN dan WLAN yangmelakukan penangkapan paket secara real-time, memonitoring jaringan, analisis protokol,mendalami paket decoding, dan diagnosis. Ini menyediakan visibilitas yang komprehensif,membantu administrator jaringan atau network engineer agar cepat menentukan danmenyelesaikan masalah berbagai aplikasi, dan karena itu meningkatkan pengalamanpengguna akhir dan menjamin lingkungan jaringan produktif. Capsa adalah alat jaringan yang bagus untuk membantu menurunkan biaya TI, meningkatkan keamanan jaringan, meningkatkan layanan pelanggan, dan lebih lincah